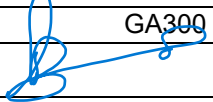


Policy #	GA300
Approved by:	
Name:	Scott Briggs
Title:	Vice President, Digital Innovation & Chief Information Officer
Approval Date:	April 5, 2022
Policy Holder:	Director, Digital Solutions
Administrative Contact:	Manager, Client Support
Replaces Policy Dated:	June 18, 2012
Review Date:	Five Years from Approval Date

Acceptable Use Policy for Digital Services

Purpose/ Rationale:

The Humber College Institute of Technology & Advanced Learning (hereafter referred to as “Humber”), in part through its “Acceptable Use Policy,” seeks to achieve the following four goals:

- a) Protect students, learners, employees, trusted partners, and guests
- b) Adhere to all applicable laws and regulations
- c) Exist within the global community as a responsible citizen
- d) Maintain the integrity and quality of digital services

This document is available in alternate format on request.

Scope:

All students, learners, employees, trusted partners, and guests of Humber and/or University of Guelph-Humber (Guelph-Humber) are required to adhere to the “Acceptable Use Policy” at all times when using Humber’s digital services either remotely or while on campus. Examples of services covered by the “Acceptable Use Policy” include network connectivity; personal computing and mobility devices; communication/collaboration tools; data storage solutions; personal productivity tools; enterprise applications; copiers/printers; and audio/visual and multimedia equipment. This policy applies to centrally managed digital services and digital services administered by Faculties/Departments. Use of any digital service, including use carried out on privately owned computing devices, is governed by the “Acceptable Use Policy.”

Definitions:

Client: Any individual or entity (includes students, learners, employees, trusted partners, and guests) using one or more digital services at Humber (also known as a “user”).

Data: Information in a raw or unorganized form (such as letters, numbers, symbols, or graphics) that refer to, or represent, conditions, ideas, or objects.

Employee: Any individual (not an independent business) providing value to Humber on a regular or semi-regular basis in exchange for compensation (wages or salary).

Guest: Any external entity (member of the public, retiree, event attendee, prospective student, alumnus, volunteer, varsity team member, etc.) interacting with Humber and/or Guelph-Humber.

Information: Timely and accurate data organized and presented in a way that gives it meaning/relevance leading to increased understanding or reduced uncertainty.

Learner: Any individual actively engaged in non-post-secondary studies (certificates, workshops, micro-credentials, rapid skills courses, bridging programs, etc.) at Humber.

Personal Use: Any activity unrelated to Humber's mission or instructional, academic, administrative, and/or research objectives (also known as a "non-Humber activity").

Service: The action of helping or doing work for someone; contribution to the welfare of others; work performed on behalf of another; activities that deliver value by enabling outcomes.

Student: Any individual actively enrolled in one or more post-secondary courses linked to a Humber and/or Guelph-Humber apprenticeship, certificate, diploma, or degree program.

Trusted Partner: An independent business providing goods and/or services to Humber in exchange for payment (also known as a "supplier", "vendor", "contractor", and/or "consultant").

Policy:

1. General

- 1.1. Clients are required to follow the law and abide by all Humber policies, standards, and guidelines when using any of Humber's digital services.
- 1.2. Digital services are made available to Clients, as appropriate, in support of Humber's mission and are intended for academic, administrative, and/or research purposes.
- 1.3. Any activity that could impact the fair, safe, and productive use of digital services or negatively impact Humber's operations, assets, and/or reputation is prohibited.
- 1.4. At all times and without exception, Clients are required to conduct themselves in an appropriate, professional manner when using any of Humber's digital services.
- 1.5. Clients are accountable for all activities logged against their credentials (username and password) or electronic signature code (including all misuse or illegal activity).
- 1.6. Use of any Humber digital service implies a Client has read the "Acceptable Use Policy" and unconditionally agreed to abide by all terms and conditions at all times.

2. Identity/Access

- 2.1. Clients are to access digital services only using the Humber credentials (username and password) assigned to them. Use of another Client's credentials is prohibited.
- 2.2. Humber usernames and passwords are personal identifiers equivalent to a signature on a document and should never be shared or disclosed to anyone at any time.
- 2.3. Humber leverages multifactor authentication as a method of protection. Clients may be required to engage in additional steps beyond the login process to access a service.
- 2.4. Clients are responsible for registering themselves for multifactor authentication. Assistance is available via the I.T. Support Centre.
- 2.5. Concealing one's identity when accessing a digital service is prohibited. Similarly, masquerading or impersonating another individual is also prohibited.

3. Prohibited Activities

Clients may not use (or allow anyone else to use) any Humber digital service to:

- a) violate any law or encourage others to violate any law
- b) conduct fraudulent activity
- c) infringe upon the rights of others
- d) threaten, incite, promote, or encourage violence, terrorism, or other serious harm
- e) impede, interfere, impair, or otherwise cause harm to the activities of others
- f) partake in any content or activity that promotes child sexual exploitation or abuse
- g) monitor or scan networked resources unless authorized
- h) intrude into the networks, systems, data files, or computing devices of others
- i) eavesdrop on others (aka a sniffing or snooping attack)
- j) use, access, or disclose others' information without authorization
- k) edit or delete one's own Humber record(s)
- l) install, use, or distribute software for which one does not have a license
- m) monitor another person's activities unless authorized
- n) create, view, collect, or share pornographic, offensive, or indecent images
- o) create or distribute malware or other disruptive/destructive constructs
- p) create or distribute ransomware
- q) violate the intellectual property rights of another individual
- r) seek to learn or use another person's credentials (username or password)
- s) impersonate a person (authority delegation facilitated by software is permitted)
- t) operate a for-profit/commercial or non-profit business without authorization
- u) distribute bulk mail (spam) or other messages for non-Humber purposes
- v) suggest Humber's endorsement of any political candidate or ballot initiative
- w) advocate for interests that are in conflict with Humber's interests
- x) waste bandwidth, server time, storage space, printer paper, or other resources
- y) compromise Humber's legitimate interests

Temporary exemptions may be granted by the Vice President, Digital Innovation & Chief Information Officer for academic, business, and/or research purposes in consultation with the appropriate (Senior) Vice President, Vice Provost, Senior Dean, and/or Director.

4. Teaching/Research

Humber's digital services may be used as a resource in support of teaching/learning and research but may not be used as a subject for teaching/learning and/or research purposes (examples: DoS and DDoS attacks, phishing attacks, man-in-the-middle (MITM) attacks, DNS spoofing, brute force attacks, session hijacking, drive-by attacks, Web attacks, eavesdropping, XSS attacks, ransomware, password attacks, SQL injection attacks, etc.) without Vice President, Digital Innovation & Chief Information Officer approval.

5. Copyright

No person shall use Humber's digital services to access, modify, distribute, and/or reproduce copyrighted material for any purposes whatsoever that is not in accordance with the Copyright Act, Humber policy (namely the Copyright Policy and the Fair Dealing Policy), and/or the terms of an appropriate license. Where there is a conflict between a license and the Copyright Policy and/or the Fair Dealing Policy, the terms of the license shall apply.

6. Personal Use

- 6.1 Limited use of digital services for personal use is acceptable and permitted provided that use does not violate any "Acceptable Use Policy" provision.
- 6.2 The personal use of digital services may not interfere or otherwise conflict with Humber operations or incur any additional costs for Humber.
- 6.3 Clients should use caution when using services for personal use. Data created, received, and/or stored are accessible and may be accessed by Humber at any time.
- 6.4 Humber is not responsible for non-Humber privacy/confidentiality breaches. Clients are encouraged to encrypt all personal files created, received, or stored at Humber.
- 6.5 The excessive consumption (as defined by Humber) of digital resources (network bandwidth, server time, file storage space, printer paper, etc.) is prohibited.
- 6.6 Digital services, when used for personal use, are provided "as is" and without any guarantee/warranty in the form of usability, functionality, availability, or continuity.
- 6.7 At any time and without notice, Humber reserves the right to modify any digital service. Humber may also terminate services for personal use without notice.
- 6.8 Deleting electronically stored files does not assure permanent erasure. Deleted data and information may be recoverable by Humber.

7. Humber Access

At its discretion and in accordance with applicable law, Humber may access, use, and disclose data and information in the following circumstances:

- a) as required by Federal, Provincial, or local law enforcement agencies
- b) to carry out essential Humber business functions
- c) as required to preserve/protect public health and safety
- d) where there are reasonable grounds to believe a law has been violated
- e) to investigate a breach of Humber policy
- f) to recover business data after an employee has left the organization

In such circumstances, approval is required from either the Vice President, Human Resources & Organizational Effectiveness; the Vice President, Digital Innovation & Chief Information Officer; or the Vice President, Students and Institutional Planning.

8. Electronic Monitoring

- 8.1 All digital services – including student, employee, trusted partner, and guest activity – are actively monitored and logged for security, diagnostic, and audit purposes.
- 8.2 By using a service, a Client grants Humber permission to collect, use, access, and disclose his or her personal information for “Acceptable Use Policy” purposes.
- 8.3 Data and information created, received, and/or stored at Humber may be accessed during the normal course of service maintenance, troubleshooting, and/or auditing.

NOTE: Humber continues to monitor provincial legislative and regulatory requirements related to electronic monitoring and will develop additional policies or protocols as needed.

9. Enforcement

- 9.1 Report suspected violations to the Vice President, Digital Innovation & Chief Information Officer or the Vice President, Human Resources & Organizational Effectiveness.
- 9.2 Pending an investigation, Humber reserves the right to immediately suspend a Client’s access to any and all digital services.
- 9.3 Students, learners, and employees who violate the “Acceptable Use Policy” may be subject to disciplinary action up to and including employment termination or expulsion.
- 9.4 Trusted partners and guests who violate the “Acceptable Use Policy” may have their Humber contracts terminated and/or be refused all future entry to Humber campuses.
- 9.5 Humber reserves the right, at its discretion, to permanently revoke student, learner, employee, trusted partner, and guest access to any and all digital services at any time.

- 9.6 Clients who violate Municipal, Provincial, Federal, or International law may be subject to criminal prosecution and/or civil litigation by the appropriate authorities.

10. Questions

Questions regarding the application of this policy may be directed to the Vice President, Digital Innovation & Chief Information Officer; the Vice President, Human Resources & Organizational Effectiveness; and/or the Vice President, Students & Institutional Planning.

References:

[Academic Employees Collective Agreement](#)
[Access & Privacy Policy](#)
[Academic Regulations](#)
[Code of Student Conduct](#)
[Copyright Act](#)
[Copyright Policy](#)
[Criminal Code of Canada](#)
[Data Governance Policy](#)
[Fair Dealing Policy](#)
[Freedom of Information & Protection of Privacy Act](#)
[Human Rights Policy](#)
[I.T. Security Policy](#)
[Remote Working and Telework Policy](#)
[Support Staff Collective Agreement](#)